ROBOT-FACILITATED CRIME

Beatrice Panattoni *

Discourse on robotics and artificial intelligence (AI) often emphasizes the benefits of these technologies. Discussion of their potential misuse in criminal activities is limited. As the capabilities of robotics and AI expand, so does their potential to facilitate crime. Specifically, the embodiment of robots introduces a unique potential for harm, as they can inflict physical damage directly. One key motivation for enhancing AI capabilities, particularly through automation and data processing, is to improve efficiency and decision-making. However, these very enhancements also increase the quantitative and qualitative harms of AI-assisted crime. If the harm is enhanced when the crime is committed in a specific way, legislations might need to take into consideration policies that enhance the punishment for certain crimes when committed with AI. In response to this growing threat, countries like Italy have proposed bills to address AI-related crime. Proposed policies draw on deterrence and punishment theories, recognizing that effective prevention requires not only technological safeguards but also a robust legal framework that sets clear penalties for AI-assisted crime. Enhancement of punishment cannot, however, be a general answer to every crime committed with robots or AI, responses should rely on a case-by-case analysis that considers the social impact of various criminal offenses relevant in the context of robot-facilitated crime. To address robot-facilitated crime in a proportionate way, scholars and international and domestic policymakers should start considering whether current criminal legislation is up to the task or if it needs updating.

INTRODUCTION

When people think about robotics and crime, they often envision a robot committing a crime. However, what is particularly interesting—and surprisingly under-theorized—is the use of robotics in facilitating crime. Such criminal

* Author's note.

phenomena might become highly relevant to contemporary society soon, yet they are largely overlooked in academic discourse.

In recent works, scholars have primarily focused on abuses against robots, [1] while comparatively little attention has been given to crimes committed through robotics.[2] Nevertheless, as will be demonstrated later, these two areas of inquiry can be closely intertwined.

The paper argues that policymakers and scholars must begin evaluating which criminal policies are most appropriate for addressing this emerging issue. While it may be premature to implement such policies, it is essential to lay the groundwork and be prepared for their potential application. The paper advocates for an integrated methodological approach that critically examines the merits and limitations of two specific criminal policy responses: the enhancement of penalties and the criminalization of new offenses.

Just as legal systems have introduced enhanced penalties for specific aggravating factors—such as complicity or the use of weapons—there may be a need to consider similar enhancements for crimes committed using robotics. However, this should not apply indiscriminately to all crimes but rather to those that meet specific criteria, as established by theories of criminalization and punishment.

Drawing on punishment theories and a recent Italian legislative proposal, the paper explores the emerging issue of robot-facilitated crime. It examines the conditions under which enhanced penalties could serve as an effective criminal policy response and considers whether alternative approaches, such as the criminalization of new offenses, might be more appropriate. The paper does not aim to provide a definitive answer to the question of what constitutes a robot-facilitated crime, or which criminal policies governments should adopt to address this phenomenon. Rather, it seeks to initiate a discussion on the issue, highlighting the legislative approaches that could be followed to address it.

The paper is structured as follows: Part I first delineates the scope of the analysis by focusing on robotics as a specific technological category. It then assesses the potential impact of robotics on crime and examines how policymakers might respond, outlining the criminal policy approaches of enhancing penalties and criminalizing new behaviors. Part II evaluates the implications of robotics for criminal policy, analyzing the opportunities and challenges associated with each approach. Finally, it considers the appropriate role of criminal law in addressing and preventing robot-facilitated crime.[3]

---

[1] Kate Darling, *The New Breed. What our history with animals reveals about our future with robots* (New York: Holt Publishing, 2021); Kamil Mamak, *Robotics, AI, and Criminal Law. Crimes against robots* (New York: Routledge, 2024).

[2] More broadly, on crimes realized with AI, see Thomas C. King *et al.*, "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions" (2020) 26 Science and Engineering Ethics 89 at 94 ff.; Keith J Hayward & Matthijs M Maas Maas, "Artificial intelligence and crime: A primer for criminologists" (2020) Crime Media Culture 1 at 6; Ugo Pagallo, "AI and bad robots: The criminology of automation", In M. R. McGuire & T. J. Holt (Eds.), *The Routledge Handbook of Technology, Crime and Justice* (New York: Routledge, 2017) 643 at 647.

[3] The paper follows the methodology proposed by Ryan Calo. See Ryan Calo, *Law and technology: a methodical approach* (Oxford: Oxford University Press, forthcoming).

I. THE IMPACT OF ROBOTS ON CRIME AND THE ROLE OF CRIMINAL LAW

Interactions within networks, where multiple actors collaborate to commit a crime, pose challenges to the allocation of responsibility. The dynamic and complex social context generated by these interactions necessitates a reconsideration of blame attribution, requiring an analysis of shared agency and the distribution of responsibility among participants based on their respective contributions to the harmful outcome. In other words, when no single criminal agent operates independently but instead acts within a shared agency framework, the constitutive elements of criminal responsibility must be reinterpreted to meet this challenge.

The legal category of complicity and criminal participation provides a primary mechanism for distributing responsibility among multiple participants in a criminal endeavor. Establishing a causal link between the harm and the actors involved is essential, with each actor's contribution determining their degree of liability. Consequently, the harm in such cases can be conceptualized as 'aggregated harm,' emerging from the broader context of these interactions.

What happens, however, when a 'participant' of the interaction is a robot, when a fragment or the whole *actus reus* is delegated to an artificial agent?

The advancement of artificial intelligence (AI) and robotics enables the delegation of certain aspects of social interactions, raising the possibility that such delegation might also occur in 'criminal interactions'—that is, interactions whose outcomes constitute criminal offenses. When a crime occurs within these interactions, the configuration of criminal responsibility is influenced by each agent's contribution. The most complex scenario arises when no human actor possesses an intention to cause harm.

A growing body of legal scholarship has begun to explore how criminal responsibility should be assigned in cases where AI-human interactions lead to unintended harm.[4] Two key areas of inquiry have been self-driving cars[5] and medical robots[6], where the potential for physical harm raises concerns of manslaughter or negligent physical injury from a criminal law perspective. However, while significant attention has been devoted to unintentional harm, less research has been conducted on intentional crimes committed through robotic agents, even though intentional harm should be the primary concern for criminal

[4] See Sabine Gless, Emily Silverman & Thomas Weigend, "If Robots Cause Harm, Who Is to Blame? Self-driving Cars and Criminal Liability" (2016) 19:3 New Criminal Law Review 412 at 424; Monika Simmler, "Responsibility gap or responsibility shift? The attribution of criminal responsibility in human–machine interaction" (2023) Information, Communication & Society 1 at 6; human-robots interactions; Elina Nerantzi Elina & Giovanni Sartor, "Hard AI Crime': The Deterrence Turn' (2024) 20 Oxford Journal of Legal Studies 1 at 2.

[5] See Gless, *supra* note 4; Marta Bo, "Are Programmers in or out of Control? The Individual Criminal Responsibility of Programmers of Autonomous Weapons and Self-Driving Cars", In Sabine Gless & Helena Whalen-Bridge (Eds.), *Human-Robot Interaction in Law and Its Narratives. Legal Blame, Procedure, and Criminal Law* (Cambridge: Cambridge University Press, 2024) 23-48; Alice Giannini & Jonathan Kwik, "Negligence Failures And Negligence Fixes. A Comparative Analysis of Criminal Regulation of AI and Autonomous Vehicles" (2023) 34 Criminal Law Forum 43-85.

[6] See Mario Verdicchio & Andrea Perin, "When Doctors and AI Interact: on Human Resposibility for Artificial Risks" (2022) 35:11 Philosophy and Technology 1-28.

law. The use of robots by human agents to commit intentional crimes remains relatively unexplored, primarily due to the lack of reported cases.

Scholars, however, have cautioned that robots might be involved in various criminal activity. For instance, robots might be purposefully used to spy on other persons or to destroy a certain target remotely.[7] Drug traffickers could use unmanned vehicles to improve smuggling success rates.[8] Another significant concern relates to the possible use of robots to commit terrorist attacks, as 'weapon of mass destruction,' which might improve in effectiveness also by combining robotics with facial recognition technologies to targeting the attacks.[9]

Given the largely speculative nature of robots' involvement in criminal activities, a natural question arises: why is it necessary to investigate robot-facilitated crime at this stage?

The answer lies in what fundamentally distinguishes robots from previous technologies—their potential impact on human experiences. When these experiences manifest as criminal acts, robots may significantly influence the nature and consequences of crime, thereby necessitating updates to crime prevention and law enforcement strategies.

Before examining the implications of this technology for legal institutions and criminal policy, it is therefore needed to first outline which robots' impacts on human experiences might be significant from a criminal law perspective, as these impacts form the foundation of the analysis.

This paper does not aim to provide a definition of robots. Instead, we refer to AI-driven systems embedded in cyber-physical bodies that –according to the 'sense, think, act' paradigm– can sense their environment, process collected information, and directly act upon their environment.[10] As such, robots function as artificial cyber-physical entities that operate within society, assuming the role of social actors when deployed in real-world environments and engaging in social interactions.

The impact of robots on human experiences is shaped by two interconnected dimensions: on one hand, their intrinsic characteristics and essential qualities,[11] on the other hand, how people interact with these machines.[12] These dimensions are

---

[7] Susanne Beck, "Google Cars, Software Agents, Autonomous Weapons Systems – New Challenges for Criminal Law?", In Eric Hilgendorf & Uwe Seidel (Eds.), *Robotics, Autonomics, and the Law* (Baden-Baden: Nomos, 2017) 227 at 231.

[8] Noel Sharkey, Marc Goodman & Nick Ros, "The coming robot crime wave" (2010) 43 IEEE Computer Magazine 114 at 116. Europol has warned about the potential use of automated drones to facilitate drug trafficking. See Report of European Monitoring Centre for Drugs and Drug Addiction and Europol, EU Drug Market: Cannabis — Trafficking and supply (2023) available at < https://www.emcdda.europa.eu/sites/default/files/pdf/31261_en.pdf?768940> (accessed March 2025). Also, in Spain, criminal organizations used drones to send drugs across the strait of Gibraltar. See The Guardian, Spanish police seize underwater drones designed to carry drugs, 4 July 2022, available at <https://www.theguardian.com/world/2022/jul/04/spanish-police-seize-underwater-drones-designed-to-carry-drugs> (accessed March 2025).

[9] See Hayward & Maas, *supra* note 2, at 6; Deane Baker, *Should we ban killer robots?* (Cambridge: Polity Press, 2022) at 28. Robots might also be used for burglary. See Ryan Calo, "Robots in American Law" (2016) 4 University of Washington School of Law Research Paper 1 at 20.

[10] Ryan Calo, "Robotics and the Lessons of Cyberlaw" (2014) 103: 3 California Law Review 513 at 529.

[11] *Id.* at 532.

[12] Jack Balkin, "The Path of Robotics Law" (2015) 6 California Law Review at 46.

intertwined. A robot's inherent qualities influence the nature of interactions, just as the experience of interacting with a robot can, in turn, shape societal perceptions of its technological attributes.[13]

Sophisticated, multi-purpose robots possess qualities that enable them to perform a wide range of operations, with their specific functions often determined by how human agent interpret and use them. A robot may be perceived and interacted with variously, as a harmless artificial entity, a pet-like companion, a delivery machine, or even a weapon. Consequently, although robots may execute tasks that resemble human actions—such as delivering packages—the fluid nature of human-robot interactions alters the overall process, introducing new capabilities. For example, a robot can deliver an item while the human agent simultaneously performs additional tasks such as real-time monitoring of multiple deliveries or surveilling the delivery perimeter.

The emergence of human-robot interactions may thus create new ways to commit crimes, whether through the delegation of unlawful tasks by human operators or through robots' ability to act autonomously. Robotics enables perception and action at a distance and presents the possibility of autonomous decision-making, problem-solving, and even social interaction.

Robots may influence criminal activities in multiple ways: they might enhance or diversify criminal methods, obscure the identification of perpetrators due to task delegation to artificial agents, and lower the psychological barriers—such as empathy—that typically inhibit direct harm to victims.

For these reasons, it is necessary to start examining the potential implications of human-robot interactions in the context of criminal activity.

However, given the current stage of technological integration, with robotic systems not yet widely distributed in society, it may be premature to implement specific legislative measures addressing robot-facilitated crimes. Nonetheless, some governments have already begun proposing legal frameworks that consider not only robotics but more broadly AI as a means to commit crime. Italy, for instance, serves as a case study in this regard, shedding light on the intersection between criminal law and emerging technologies.

A. The harms of robot-facilitated crimes

One of the first issues that may arise, given the new capacities enabled by AI and robotics, concerns the extent to which these technologies, when exploited for criminal activity, may amplify the harm resulting from such offenses. Specifically, a key question is whether the harm caused by a crime facilitated by a robot would be more severe than the harm caused by the same crime without the robot's involvement. Indeed, robots and AI may exacerbate the impact of existing offenses, or create new threats, raising the need to reform existing criminal offences or to criminalize new forms of behavior.

[13] See Mark Coeckelberg, "Is Ethics of Robotics about Robots? Philosophy of Robots Beyond Realism and Individualism" (2011) 3:2 Law, Innnovation & Technology 241; Mark Coeckelberg, *Robot Ethics* (Cambridge: The MIT Press, 2022). Coeckelberg stresses that 'what a robot 'is' is always shaped by human use, (inter)action, subjectivity, and culture'. At the same time, technology affordances, which derive from how the technology is designed, can shape human behavior. See David Collingridge, *The social control of technology* (New York: St Martin's Press, 1980).

To address these challenges, it is essential to understand the nature and extent of harms that may emerge from robot-facilitated crime. However, given the scarcity of real-world cases, it is still too early to conduct a comprehensive analysis or develop a taxonomy of the specific areas of crime in which robots may be involved.

Broadening the perspective from robots to AI, the risks posed by AI systems are quite wide. As illustrated by the banned AI systems under the European AI Act,[14] these risks include, for instance, psychological and economic harm. Consider the case of manipulative AI systems that exploit users' cognitive vulnerabilities through subliminal techniques, which may intensify both the scale and severity of harm of manipulative behaviors.[15]

The increasing sophistication of machine learning allows AI to conduct advanced data analysis and predictive modeling, which criminals can exploit for malicious purposes.[16] The function of these systems, combined with the profiling of users, can improve the effectiveness of the manipulative process. Furthermore, large-scale AI-driven manipulative interactions—such as targeted psychological manipulation of specific groups—could be weaponized by criminal actors to conduct attacks at an unprecedented scale.

Conversely, EU policymakers do not seem to have explicitly considered robots and physical harm in the list of banned AI systems. However, the embodiment of AI in robotic systems might introduce a distinct risk of direct physical harm. Unlike purely virtual AI systems, robots possess a physical presence that allows them to interact with and potentially cause harm to human bodies. Therefore, physical harm is a primary concern when assessing the risks associated with robots. This is not to suggest that other forms of harm—such as psychological or economic harm—are irrelevant. However, physical injury caused by robots carries particularly strong social implications, influencing public perception of robots as autonomous agents operating safely within human environments. Addressing these concerns is crucial, as it directly affects trust in human-robot interactions and the overall trustworthiness of robotic technologies in society.

When a person is harmed by a robot, it reinforces perceptions of technological danger and raises concerns about deterrence and prevention. Therefore, beyond direct individual harm, another relevant dimension must be considered: the impact on public trust in robotics. If robots are used to commit crimes, this could undermine their acceptance as safe and beneficial artificial agents. Regulatory frameworks are designed to ensure the responsible development and deployment of robotic technologies, but their involvement in

[14] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence (Artificial Intelligence Act).

[15] See ANNEX to the Communication to the Commission Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), Brussels, 4 February 2025, C(2025) 884 final.

[16] For instance, AI might be used to organize 'Online influence operations', covert or deceptive efforts to influence the opinions of a target audience. See Josh A. Goldstein *et al.,* "Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations" (2023) Joint report with Georgetown University's Center for Security and Emerging Technology OpenAI and Stanford Internet Observatory. Advance online publication. arXiv:2301.04246.

crime could weaken public confidence in these safeguards. Moreover, robots' physical presence in the environment makes them more visible and tangible participants in criminal acts, particularly when they interact directly with humans or other systems. This embodied nature alters their affordances, allowing them to influence and modify real-world situations in ways that virtual AI systems cannot. Additionally, their role in criminal activities—particularly when they seemingly contribute to the *actus reus*—may blur the distinction between tool and accomplice, raising complex legal and ethical questions.

However, one fundamental principle must be clarified: robots cannot be criminals or criminal accomplices. The idea of assigning direct criminal responsibility to robots— even when shared with a human agent through the legal institution of complicity[17] —is widely contested among legal scholars, as it conflicts with established principles of criminal law.[18] Criminal responsibility requires a moral agent—an entity capable of consciousness, understanding, and moral reasoning.[19] Since robots lack these qualities, holding them directly accountable for crimes is not a viable approach.[20]

Nevertheless, to say that robots cannot have moral status does not imply they do not deserve moral or, better yet, ethical consideration. When involved in criminal activities, the intervention of criminal law must consider not only the human actions, but the human-robot interactions, assessing and evaluating whether criminal offences and policies are adequate to contain their impacts. Therefore, since direct criminal responsibility of robots does not constitute a valuable option, criminal policies must explore alternative approaches and assess whether existing legal frameworks are sufficiently armored to address robot-facilitated crimes.

B. Criminal reforms

As briefly mentioned above, policymakers may adopt two distinct approaches to criminal policy in response to robot-facilitated crime: (1) enhancing penalties for existing offenses and (2) criminalizing new behaviors. The latter category can also include policies that ban specific types of robots when their creation, commercialization, or deployment is prohibited under criminal law.

---

[17] One of the few scholars who are open to the possibility of direct criminal responsibility of AI, also as accomplince of a crime, is Hallevy. See Gabriel Hallevy, *When Robots Kill: Artificial Intelligence under Criminal Law* (Boston: Northeastern University Press, 2013) 75.

[18] The majority of scholars reject the idea of directly punishing AI systems based on classical criminal law principles. See Ryan Abbott & Alex Sarch, "Punishing Artificial Intelligence: Legal Fiction or Science Fiction" (2019) 53: 1 UC Davis L Rev 323 at 327; Dafni Lima, "Could AI Agents Be Held Criminally Liable? Artificial Intelligence and the Challenges for Criminal Law" (2018) 69 South Carolina Law Review 677 at 679; Gless, *supra,* note 4, at 417; Peter Asaro, "A Body to Kick, but Still No Soul to Damn: Legal Perspectives on Robotics", In P. Lin, K. Abney, & G. Bekey (Eds.), *Robot Ethics: The Ethical and Social Implications of Robotics* (Cambridge: The MIT Press, 2012) 169 at 181.

[19] Some scholars suggest the need to start framing a "new branch" of "punitive law" dedicated to crimes realized by AI. See Nerantzi & Sartor, *supra* note 4.

[20] Additionally, the problematic comparison of robots to people could lead to neglecting the accountability of those who create them. See Darling, *supra* note 1, at 83.

To examine and evaluate the rationale and critiques of these criminal policies, this paper will refer to a recent report by the *Association Internationale de Droit Pénal* (AIDP). The most recent AIDP international congress focused on AI and criminal law, leading to the publication of reports prepared by experts from several Countries around the world. These reports address four key areas: (1) AI and criminal law theory, (2) AI-related offenses, (3) AI and criminal procedure, and (4) AI and international criminal law. The second report—on AI-related offenses—is particularly relevant to the scope of this paper, given that it considers both policy approaches.[21]

The first approach is based on the premise that the enhanced capabilities enabled by robots can lead to an increase in potential harm, thereby justifying harsher penalties. A notable case study illustrating this perspective is the Italian legal system, where the government recently published a bill addressing the implications of AI—including but not limited to robots—on the criminal justice system.[22]

The Italian bill adopts a criminalization approach that is limited to what, in the policy makers perspective, constitute most alarming behaviors. The promised limitation of the intervention should prevent the risk of stigmatizing AI itself, intervening only in cases of unlawful use of AI systems—specifically those that cause harm or pose a threat to legally protected interests, including constitutionally relevant ones.

The bill, according to Articles 22 and 25, is structured along four main lines of policy. (1) Establishing mechanisms to prevent the dissemination and remove content illicitly generated using AI systems. (2) Defining one or more new independent criminal offenses, punishable by intent or negligence, centered on the failure to adopt or update security measures for the production, circulation, and professional use of AI systems. (3) Defining one or more new independent criminal offenses, punishable by intent, aimed at protecting specific legal interests at risk due to the use of AI systems, which cannot be adequately safeguarded under existing legal provisions. (4) Introducing aggravating circumstances—specific ways of committing a crime that exacerbate its harm and, consequently, warrant harsher penalties.

For the purposes of this paper, the most relevant aspect is the fourth criminal strategy, as the third pertains solely to the creation of a new criminal offense related to the production of fake sexually explicit materials using AI systems without the consent of the depicted individual (commonly known as deep nudes). As a result, robots are not expressively considered within the policies of criminalization new behaviors.

Instead, it is particularly valuable to examine more closely the proposed introduction of aggravating circumstances. The Italian bill suggest adding to the Italian Criminal Code, specifically: (4a) A common aggravating circumstance for all crimes. (4b) Special aggravating circumstances for certain crimes.

---

[21] See Fernando Miró-Llinares, Constantin Duvac, Tudorel Toader & Mario Santisteban Galarza (Eds.) *Criminalisation of AI-related offences* (2024) 1 Revue Internationale de Droit Pénal 1-445.

[22] Italian Bill n. 1146 presented 20 May 2024, on provisions and delegation of authority to the government on artificial intelligence.

The common aggravating circumstance would apply to all crimes, increasing penalties when the offense is committed using AI systems, provided that their nature and method of use constituted a 'deceptive means' or hindered public or private defense, or worsened the consequences of the crime. A 'deceptive means' refers to a method capable of distorting reality and deceiving the victim due to its deceptive potential. It involves a behavior or a tool that, by its misleading nature or the circumstances of its use, poses a hidden danger that catches the victim off guard (such as a sudden swerve of a car driven by the victim). Special aggravating circumstances, on the other hand, would apply only to specific crimes where AI systems, according to the Italian policy makers, 'clearly amplify the impact of the offense'. The penalty would be increased simply for committing certain crimes through AI, such as identity fraud, fraud, market manipulation, money laundering, and copyright infringement.

The Italian case present an example of the first criminal policy outlined, which consider the enhancement of penalties of existing criminal offences. The second policy described pertains to the introduction of new criminal offenses. In this context, criminalization could encompass the bans of certain AI systems or other dangerous behaviors when prodromic to the commission of a more serious crime. According to the AIDP report, the majority of national experts express skepticism regarding this policy, since 'from today's perspective, robot systems—even if they were to be self-learning—should not be rated any differently than other machines.'[23] Although, according to certain scholars, 'to guarantee an adequate level of legal protection, the criminal justice system might need to resort to the anticipation of the criminal protection. As happened before with cybercrime, the need to criminalize conducts that are prodromic to the realization of a more harmful crime might emerge.'[24] Currently, no national legislation provides a case study specifically on the criminalization of crimes facilitated by robots[25]. Nevertheless, criminalization might be an alternative policy to the enhancement of penalties, warranting careful examination.

In the next section, we will examine both the opportunities and the critiques of these two criminal policies.

II. ASSESSMENT OF CRIMINAL POLICIES

In assessing the two outlined criminal policies, certain principles of criminal law must serve as the foundation for argumentative reasoning. The first is the principle of legality. Overly broad criminal offenses do not adhere to the strict principle of legality, which requires that the description of criminal behavior be clear and precise. To avoid overcriminalization—particularly given that robotics is a multi-purpose technology applicable across various fields—criminal policies

[23] See Miró-Llinares, *supra* note n. 21, at 44.

[24] Id. at 188.

[25] There are relevant examples in the broader context of AI regulation. For instance, article 33 of the French law 2019-222 (*Réforme pour la justice*) has modified article L10 of the *Code de Justice Administrative*, to, among other measures, criminalize the use of AI to predict a court decision, by punishing the use of «the identity data of magistrates and members of the registry (…) for the purpose or effect of evaluating, analyzing, comparing or predicting their actual or supposed professional practices». See Miró-Llinares, *supra* note n. 21, at 45.

aimed at addressing crimes involving robots must refrain from using excessively broad language to define their involvement. In framing this concern, the experience gained in the fields of computer crime and cybercrime—where criminal law first began to address the role of computer science in the commission of offenses—can provide a useful reference to guide criminal policies.

The second issue to consider is the legitimation of criminal law in the formulation of these criminal policies. The expansion of criminalization and the enhancement of punishment must be justified within the framework of the principle of proportionality, ensuring that the severity of the punishment corresponds appropriately to the gravity of the crime.

A. The lessons of computer crime and cybercrime

When introduced into criminal justice systems, computer crime and cybercrime brought forth a series of criminal offenses in which the technological component—information technology (IT) and information and communication technology (ICT)—became a 'constitutive' element of the crime.[26] Without technology, these specific offenses could not exist, as they derive directly from the misuses and abuses of digital systems. For instance, the crime of illegal access to a protected ICT system (illegal hacking) originates from interactions between technological infrastructures and criminal agents. Without computers, hacking as a criminal offense would not be conceivable.

At another level, as society undergoes increasing digitalization, a growing number of crimes can now be committed through computers or in cyberspace. However, this shift does not necessarily necessitate the creation of new, 'digitalized' offenses to address technologically facilitated crimes. For example, while stalking is now frequently carried out online, cyberstalking does not constitute a distinct criminal offense but rather represents a new means of committing an existing crime. Crimes evolve in response to technological advancements and societal changes, requiring legal frameworks to be updated when necessary. However, the mere advancement of technology does not itself justify the criminalization of new behaviors.

In this context, a two-pronged framework emerges. On one hand, certain offenses can only exist due to technology. The crimes which explicitly require a technological component are, resorting to the terminology under the United Nations Convention on Cybercrime,[27] 'cyber-dependent crimes'. Such offenses are inherently linked to technology, with legal definitions explicitly addressing the misuse of technological systems. On the other hand, technology can function merely as a means to commit an already recognized offense. These crimes, named

---

[26] On computer crimes, see Donn B. Parker, *Crime by computer* (New York: Scribner, 1976); Orin Kerr, *Computer Crime Law*, n° 5 ed. (US: West Academic Publishing, 2022); on cybercrime see Alisdair Gillespie, *Cybercrime. Key issues and debates* (London: Routledge, 2019); David Wall, *Cybercrime. The transformation of crime in the Information Age*, n° 2 ed. (Cambridge: Polity, 2024).

[27] United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes, adopted by the General Assembly of the United Nations on 24 December 2024 in New York by resolution 79/243.

as 'cyber-enabled crimes' under the same UN framework, may involve aggravating circumstances when technology does not represent the more frequent way of commission—as a result of the crime evolving in society—but it is used in an exceptional and particularly harmful manner. For instance, if the technological means of committing a crime significantly amplifies its severity compared to its traditional form, additional legal considerations may arise.

This distinction raises the question of whether AI-driven offenses should be following the same path. Unlike robotics, which primarily involves physical systems, AI technologies—such as deepfakes—are already widely accessible online. Certain harms facilitated by AI, such as the creation and distribution of deepfake pornography (e.g., deep nudes), would not be possible without AI. In such cases, criminalization targets the distribution of artificially generated content, as seen in recent legislative initiatives, such as the Italian bill addressing deepfake-related offenses. At the same time, as proposed in the Italian bill, AI can be considered a specific means of committing an existing crime, warranting aggravating circumstances. This applies not when AI becomes the most common method of perpetrating the crime, but rather when it constitutes a specific, more severe way of committing it.

The field of computer crime and cybercrime offers additional insights into broader legal and policy considerations. First, advancements in ICTs have necessitated a focus on preventive criminalization, targeting behaviors that precede the commission of more serious crimes. For example, the illegal distribution of malware capable of damaging computer systems is criminalized because it facilitates subsequent offenses involving system breaches and destruction.[28]

Second, the transnational nature of cybercrime highlights the necessity of international cooperation in criminal policy. While law enforcement and legal competencies remain primarily within national jurisdictions, the role of international organizations, such as the United Nations, is crucial in coordinating policies across states. Effective enforcement strategies require an integrated and relatively uniform international framework. For example, the previously mentioned United Nations Convention against Cybercrime seeks to harmonize global efforts against cybercrime. However, a notable gap in this convention is its lack of provisions addressing AI-related crimes.

In summary, three key lessons emerge from the experience of computer crime and cybercrime: (a) lawmakers can legally frame technology's role in criminal offenses either as a tool for committing existing crimes or as the

[28] The Convention of the Council of Europe signed in Budapest, 23 November 2001, required the States to introduce criminal offences of misuse of devices. According to its Article 6: 'Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5 (illegal access, illegal interception and illegal damage of computer data, programs, systems); a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5 (…)'.

foundation of technology-dependent offenses; (b) legal systems may need to criminalize preparatory behaviors that could lead to more serious harm; and (c) the coordination between national and international legal frameworks is an essential element to ensure effective law enforcement in the digital age.

B. The principle of proportionality as scale to measure criminal policies

To assess whether both enhancement of penalties and criminalization are sufficiently legitimate as criminal policy choices, they must be subjected to the scrutiny of the principle of proportionality.

This principle serves as a legal tool for achieving an appropriate balance between competing interests. In criminal law, the principle of proportionality operates on multiple levels. The most widely recognized and studied is the judicial level, where the proportionality of punishment in sentencing has long been a central issue in criminal law theory and philosophy.[29] However, this principle also plays a crucial role at the legislative level. When policymakers decide to reform substantive criminal law—whether by modifying penalties or introducing new crimes—the principle of proportionality must guide their decisions.

To provide a definition, 'for contemporary legal orders proportionality is a definable concept but not necessarily a 'measurable' one. Depending on the context, it is usually recognized as a criminal law principle guaranteeing a relationship between offence and punishment that is 'just', a practical optimization rule or guiding principle for facilitating the balancing between competing interests and/or a checks-and-balances tool and legal reasoning technique for (constitutionally) assessing the restriction of fundamental rights.'[30]

Thus, both enhancement of penalties and criminalization must be proportionate to be considered legitimate. The key challenge lies in determining the relata of proportionality. While it is widely accepted that punishment must be proportionate to the 'seriousness' of the offense,[31] the concept of seriousness can be interpreted from multiple perspectives.

---

[29] See, Youngjae Lee, "Why Proportionality Matters" (2012) 160 University of Pennsylvania Law Review 1835; Thomas J. Miceli, "On Proportionality of Punishments and the Economic Theory of Crime" (2018) 46 European Journal of Law and Economics 303; Jasper Ryberg & Julian V. Roberts (Eds.), *Popular Punishment. On the Normative Significance of Public Opinion* (Oxford: Oxford University Press, 2014); Andrew von Hirsch, *Deserved Criminal Sentences* (Oxford: Hart Publishing, 2017); Andrew von Hirsch & Andrew Ashworth, *Proportionate Sentencing: Exploring the Principles* (Oxford: Oxford University Press, 2005).

[30] Emmanouil Billis & Nandor Knust, "Proportionality (Principle of)", In Pedro Caeiro *et al.* (Eds.), *The Elgar encyclopedia of crime and criminal justice* (Northampton: Elgar Publishing, 2024) 234. See also Emmanouil Billis, Nandor Knust & Petter Rui, "The Typology of Proportionality", In Emmanouil Billis, Nandor Knust & Petter Rui (Eds.), *Proportionality in Crime Control and Criminal Justice* (Oxford: Hart Publishing, 2021) 21; Michael Bothe & Emanuela-Chiara Gillard, "The Proportionality Principle in Comparative Public, European Union and International Law – Reflections on the Proportionality Equation", In Emmanouil Billis, Nandor Knust & Petter Rui (Eds.), *Proportionality in Crime Control and Criminal Justice* (Oxford: Hart Publishing 2021) 277.

[31] Mitchell Berman, "Proportionality, Constrain, Culpability" (2021) 15 Criminal Law and Philosophy 373 at 375; Matt Matravers, "The place of proportionality in penal theory: or rethinking about punishment", In Michael Tonry (Ed.), *Of One-eyed and Toothless Miscreants: Making the Punishment Fit the Crime?* (Oxford: Oxford University Press, 2019) 76.

In Anglo-Saxon and Anglo-American criminal law theory, the focus is on the 'communicative effect' of punishment,[32] where criminal responsibility is closely tied to moral culpability. In this view, disproportionate sanctions 'risk . . . of either confusing common morality or flouting it and bringing the law into contempt.'[33] Because this perspective emphasizes the communication toward the blameworthiness of wrongs, the seriousness of a crime is primarily linked to how blameworthy the conduct of the criminal agent is, to the degree of the offender's desert. This approach leans toward retributivism, as it looks back on past conducts.

However, the overlap between criminal responsibility and moral legalism risks undermining the objectivity of punishment's legitimacy. If punishment is justified primarily by an offender's moral blameworthiness, the criminal justice system may drift toward symbolic penalization aimed at neutralizing certain individuals rather than ensuring justice. Furthermore, a rigid and static retributivist framework risks becoming excessively fixated on past wrongdoing, neglecting forward-looking considerations such as prevention. At the same time, a purely consequentialist approach—emphasizing punishment's future benefits, particularly through deterrence—could justify excessively severe sanctions if they serve preventive purposes.[34]

In the perspective of 'mixed theories',[35] a past wrong is not a merely past wrong; rather, punishment becomes a rehabilitative process designed to foster social solidarity and protect rights and interests. Consequently, proportionality requires a balanced approach: a fluid present-oriented perspective that considers both past actions and future consequences, accounting for the offender, the victim, and the broader context of the crime.

Legal tradition in continental Europe adds a significant element to this reasoning, following a slightly different approach.[36] Advocating for the separation of criminal responsibility from moral considerations, its perspective frames punishment as a mechanism for protecting individual and collective rights and interests, rather than as a means of expressing moral condemnation.

Under this framework, deterrence and desert are insufficient, they must be accompanied by constitutional reasonableness. Here, the seriousness of an offense is not determined by the blameworthiness of the conduct but by the degree of harm it causes. The severity of an offense is assessed based on the rights and interests the criminal law seeks to protect.[37] This approach ensures a more objective assessment of offense severity, using the actual harm inflicted as the key parameter.

From this perspective, punishment is considered proportionate if it effectively serves the overarching aim of the criminal policy under scrutiny—

---

[32] According to this theories of punishment, criminal law is a way of communicating social values important for the community. See Anthony Duff, *Punishment, Communication, and Community* (Oxford: Oxford University Press, 2001); Joel Feinberg, "The Expressive Function of Punishment" (1965) 49: 3 The Monist 397.

[33] Herbert L. A. Hart, *Punishment and Responsibility. Essays in the philosophy of law* (Oxford: Clarendon Pr., 1968) 25.

[34] Andrew von Hirsh, "Proportionality in the Philosophy of Punishment: From "Why Punish?" to "How Much?" (1990) 2:1 Criminal Law Forum 259 at 263.

[35] See Andrew von Hirsh, *Censure and Sanctions* (Oxford: Clarendon Press, 1993).

[36] See Vittorio Manes, *Il principio di offensività nel diritto penale. Canone di politica criminale, criterio ermeneutico, parametro di ragionevolezza* (Torino: Giappichelli, 2005).

[37] Von Hirsh, *supra* note n. 35, at 15.

namely, the program of criminal protection of legally recognized interests that stays behind the specific considered criminal strategy.

C. The enhancement of penalties

The policy of enhancing penalties risks tilting the balance excessively toward deterrence. If the guiding criterion is the quantitative and qualitative aspects of harm, increasing punishment as a general approach creates a tension. On the one hand, deterrence theory—which posits that the fear of punishment can prevent crime—is particularly relevant in this context, as it underscores the importance of establishing firm consequences for crimes committed with the aid of robotics. On the other hand, an overreliance on deterrence theory risks leading to 'overdeterrence', namely, excessive penalization and questionable criminal policies based on social control through 'governing through crime.'[38]

As stated in the report of AIDP, even though AI 'might facilitate the commission of crimes and make prosecution more difficult given that the perpetrator is not required to be in the scene of the crime', 'this increased potential for harm does not necessarily require severe penalties, and the decision of modifying the penalty range shall be done in a case-by-case basis on each offence'.[39]

The primary critique of this approach concerns the introduction of a general aggravating circumstance applicable to all crimes. Even if its scope is limited by certain specifications—such as the use of AI as a deceptive tool, as a means of obstructing public or private defense, or as a factor that exacerbates the consequences of the crime—the definition remains overly broad. This ambiguity risks allowing judges to enhance penalties whenever AI or robotics are involved in a crime, leading to an unjustified stigmatization of AI itself. The concern here is the objectification of responsibility, where the mere use of AI could result in harsher punishment, irrespective of the actual role AI played in increasing harm.[40] Excessive deterrence applied too broadly and prematurely, risks imposing disproportionate punishments solely based on the assumption that they might reduce crime.

Enhancing penalties cannot serve as a blanket response to all crimes involving AI or robotics. Instead, legal responses should be tailored to individual cases, assessing the social impact of specific offenses in the context of robot-related crime.

A more reasonable approach involves introducing special aggravating circumstances where empirical and objective assessments demonstrate that robots significantly increase harm in specific crimes. This policy is more justifiable, but the crimes addressed in the current legislative proposal appear to be tailored primarily to AI systems operating online rather than physical robots. Crimes such as identity fraud, fraud, market manipulation, money laundering, and copyright infringement are not (yet) facilitated by robots.

---

[38] See Jonathan Simon, *Governing through crime. How the war on crime transformed American democracy and created a culture of fear* (Oxford: Oxford University Press, 2007).

[39] See Miró-Llinares, *supra* note n. 21, at 54.

[40] *Id.*

Moreover, caution remains necessary, as existing aggravating circumstances in many legal systems may already address such concerns. For example, in some jurisdictions, drug trafficking is considered an aggravated offense when committed using ships, boats, or aircraft, regardless of whether the aircraft is manned or unmanned.[41] Similarly, offenses such as drug trafficking carry higher penalties when they are linked to organized crime or terrorist organizations. As the AIDP report states, in these cases, 'the use of AI or drones could be punished more severely, and no amendments are required.' [42]

A possible legal gap may instead arise in cases of robot-facilitated crimes that result in death or physical injury. The enhancement of penalties for homicides or physical harm caused by robots could be justified by the increased quantitative and qualitative dimensions of harm.

From a quantitative perspective, physical harm caused by robots may pose unique dangers, such as the ability to inflict injury remotely or cause multiple injuries simultaneously, in addition to their enhanced operational capabilities. From a qualitative perspective, harm is aggravated by the human-robot interaction itself. The question then arises: What exactly should be protected? In addition to life and physical integrity, a new public interest may emerge—ensuring safety in human-robot interactions, considering robots as social artificial agents.[43]

In this context, physical harm is compounded by an additional risk: the erosion of trust in social artificial actors. Crimes committed using robots may also exploit humans' trust in robotic systems, leading to broader societal concerns. Therefore, the enhancement of penalties in such cases may be justified for deterrence purposes. From this policy perspective, criminal protection could be extended beyond physical harm to include the preservation of public trust in human-robot interactions.

D. Criminalization

Given the seriousness of physical harm that can be caused by criminals who exploit robotic systems, the policy of criminalization might follow the path of cybercrime, assessing the need to criminalize robot-dependent offenses that serve as precursors to the abuse of robotics for causing physical harm.

Since criminals may inflict physical harm by misusing robotics, safeguarding robots from abuse is a crucial first step in protecting the public from criminal human-robot interactions. Preventing such abuse is essential, as crimes involving robots might stem from their unlawful manipulation. In other words, crime 'through' robots might be the result of crime 'against' robots.

---

[41] *Id.*

[42] *Id.* at 80.

[43] See Mamak, *supra* note n. 1, at 32. Moral significance according to a 'relational approach' is based on the relations that humans can have with robots. 'Moral status emerges through social relations between different beings'. See John-Stewart Gordon & David J. Gunkel, "Moral Status and Intelligent Robots" (2022) 60:1 The Southern Journal of Philosophy 88 at 99. To establish this dimension of legal protection the parallelism with animals could be useful. See Mark Coeckelbergh & David J. Gunkel, "Facing Animals: A relation, Other-Oriented Approach to Moral Standing" 27: 5 Journal of Agricultural and Environmental Ethics 715; Darling, *supra* note n. 1, at 179.

Also in this regard, the findings of the AIDP report provide a valuable reference. The research conducted by the group of experts suggests that policymakers should consider introducing new offenses 'to punish the abuse and transformation of existing lawful AI systems when, by changing the design or the purpose of the AI, new risks arise'.[44] 'In the same way that the revolution on gene editing led to the appearance of offenses sanctioning genetic manipulation with the capacity for mass destruction, technological evolution may make it necessary, in the near future, to criminalize the creation, development and use of AI tools with a high destructive capacity, such us some autonomous weapons, drones or robots that could be enormously harmful specially if human control is lost'.[45]

Thus far, scholarly discussions have primarily focused on artificial general intelligence (AGI) rather than robotics.[46] Some proposals in the literature suggest the need to criminalize the 'introduction'—meaning 'letting in the wild', by programming or releasing into the market—of 'uncontrollable'—meaning with 'no opportunity to impact the direction in which AGI operates or to turning it off'—AGI.[47]

However, a more immediate concern might concern the criminalization of abuses against robots aimed at transforming them into weapons—namely, the 'weaponization' of robots. This could emerge as a logical extension of existing bans on autonomous weapon systems,[48] where regulations of these systems involve distinct legal considerations related to robots implemented in military settings under *jus in bello* and military law. Since general rules on liability for illegal trafficking of arms, ammunition, explosives and explosive devices may not be applicable to AI,[49] this scenario could provide the necessity to introduce a technology-dependent crime, where the concept of 'weaponization' refers specifically to the misuse of a robot's intended function, as prescribed by its designers and manufacturers, in order to convert it into a weapon.

Efforts to criminalize robot-facilitated crimes must, therefore, begin with the criminalization of abuses against robots themselves.[50] This relation can also be

---

[44] Miró-Llinares, *supra* note n. 21, at 15, number 16.

[45] *Id.* number 22.

[46] See Kamil Mamak, "AGI crimes: the role of criminal law in mitigating existential risks posed by artificial general intelligence" (2024) AI & Society, available at < https://link.springer.com/article/10.1007/s00146-024-02036-5> (accessed March 2025); David Atkinson, "Criminal Liability and Artificial General Intelligence" (2019) 2:5 Robotics, Artificial Intelligence & Law 333.

[47] See Mamak, *supra* note n. 46, at 7.

[48] Around Lethal Autonomous Weapon Systems (LAWS) have grown a wide and complex debate, relating the potential prohibition of LAWS. See Peter Asaro, "On banning autonomous weapon systems: human rights, automation, and the dehumanization of lethal decision-making" (2012) 94: 886 International review of the Red Cross, 687-709; Frank Sauer "Lethal autonomous weapons systems", In Anthony Elliott (Ed.) *The Routledge Social Science Handbook of AI* (London: Routledge, 2021) 237. See also the Special Issue of the Journal of International Criminal Justice, "Autonomous Weapon Systems and War Crimes" (2023) 21:5.

[49] See Miró-Llinares, *supra* note n. 21, at 63.

[50] While this paper primarily examined issues related to physical harm intended as harm to physical integrity, other instances of harms against the person might be related to robot-facilitated crime, which could also require legal intervention. For example, the misuse of sex robots could contribute to criminal behavior or incite certain offenses. Additionally, the protection of minors

viewed from the opposite perspective: preventing robot-facilitated crimes may serve as legitimation ground for criminalizing abuses against robots.

CONCLUSION

To address robot-facilitated crime in a proportionate manner, both international and domestic regulatory frameworks must assess whether existing criminal legislation is adequate or requires revision.

In this context, punitive and preventive strategies should complement each other. Policymakers must consider measures to deter the misuse of robotics. However, these strategies should also be balanced with preventive, non-criminal approaches, such as the development of secure AI systems with built-in anti-abuse safeguards to mitigate risks. A relevant example is the European AI Act, which highlights the importance of regulatory intervention.

The experience of IT and ICT-facilitated crime showed how the introduction of computer fraud offenses in the 1990s did not eliminate computer crime, which instead evolved in cybercrime. Enhancement of penalties and criminalization alone are rarely an effective policy; in some cases, they may even exacerbate the problem by driving offenders to become more sophisticated and harder to detect. Therefore, alternative approaches should be explored, emphasizing risk prevention and corporate cooperation.

The emergence of new robot-dependent crimes, such as weaponization of robots, might provide clearer guidance for producers and designers on the areas of risk that require mitigation. Establishing well-defined standards can clarify what must be prevented and what measures companies must implement to ensure their products are not weaponized or that weaponized robots are not misused beyond the scope of armed conflict.

A comprehensive approach that integrates regulatory, technical, and ethical strategies can help ensure that AI development progresses responsibly, balancing technological innovation with the need to protect society from robot-facilitated crime.

---

may be jeopardized by the development of sex robots designed to resemble children, raising significant ethical and legal concerns. See Mamak, *supra* note n. 1, at 76.